FILED
MAY 02 2018
U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

IN RE SEARCH OF:
Samsung, Model Number SM-J327P,
silver in color DEC: 089 869 568 800 424 053
Located at: St. Charles County Police Department,
Evidence Room, 101 Sheriff Dierker Court
O'Fallon, Missouri 63366

AFFIDAVIT

I, Detective Andrew Sitton, being duly sworn, do hereby depose and state:

Introduction

1. I am a Detective with the St. Charles County Cyber Crimes Task Force and part of the St. Louis Federal Bureau of Investigation ("FBI") Child Exploitation Task Force. I have been assigned to the St. Charles County Cyber Crimes Task Force for over one (1) year. I have investigated matters involving the online exploitation of children, particularly in relation to violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, which criminalize the production, possession, receipt, distribution and transmission of child pornography.

2. This affidavit is made in support of an application for a search warrant to search a Samsung, model SM-J327P, DEC: 089 869 568 800 424 053, cellular telephone which is silver in color, is located at St. Charles County Police Department, Evidence Room, 101 Sheriff Dierker Court O'Fallon, Missouri 63366. It was seized on April 25, 2018, by the St. Charles County Cyber Crimes Task Force from Rodney Grant SULLIVAN, residing in Missouri.

3. The statements contained in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation from others, and on my experience and background as a Detective with the St. Charles County Cyber Crimes Task Force. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A.

Statutory Authority

4. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, which criminalize, among other things, the production, possession, receipt, and shipment of child pornography, and other related materials.

Definitions

5. The following definitions apply to this Affidavit and Attachment A to this Affidavit:

a. "Child pornography" means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC § 2256(8)(A) and (C).

b. "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. 18 USC § 1030(e).

c. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including for example, tablets, digital music devices, portable electronic game systems, electronic game counsels and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, DVDs, CDs, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. “Computer passwords” and “data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

e. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

f. “Electronic data” may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

g. “Identifiable minor” means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person’s face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 USC § 2256(9).

h. The “Internet” is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between devices, such as computers and wireless phones, and other Internet capable devices, exist across state and international borders and information sent between devices connected to the Internet frequently crosses state and international borders, even if those devices are in the same state. A network is a series of devices, including computers and telecommunication devices, connected by communication channels.

i. “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses

might be static whereby the user's ISP assigns his computer a unique IP address – and that same number is used by the user every time his computer accesses the Internet. Numerical IP addresses generally have corresponding domain names. For instance, the IP address 149.101.10.40 traces to the corresponding domain name "www.cybercrime.gov." The Domain Name System or DNS is an Internet service that maps domain names. This mapping function is performed by DNS servers located throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

j. "Minor" means any person under the age of eighteen years (18 U.S.C. § 2256(1)).

k. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), wireless telephones, Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

l. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

m. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

n. "Wireless telephone" (or "mobile telephone," "cellular telephone," or "cell phone") is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the

telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Wireless telephones may also be able access various local area networks and the Internet through a Wi-Fi connection and Bluetooth technology.

Computers and Child Pornography

6. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography was formerly produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of such items was most often accomplished through a combination of personal contacts, mailings, and telephone calls.

7. The development of computers has changed the way in which individuals interested in child pornography interact with each other, as computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. Digital cameras allow images to be transferred directly onto a computer. A device known as a modem permits computers to connect to other computers through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the

last several years. These drives can store hundreds of thousands of images at a very high resolution.

10. A growing phenomenon on the Internet is peer-to-peer file-sharing (P2P).

11. The latest evolution of P2P software is a program that allows a user to set up their private P2P network of contacts. File-sharing through this new and publicly available P2P file-sharing program is limited only to other users who have been added to a private list of "friends." A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the list of files that the other user has made available to download, select desired files from this list, and download the selected files. The downloading of a file occurs through a direct connection between the computer requesting the file and the computer containing the file.

12. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

13. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

14. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

Wireless Telephones and Child Pornography

15. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, wireless telephones have likewise revolutionized the manner in which child pornography is produced and distributed.

16. Wireless telephones, also known as cellular phones or cell phones, are exceptionally widespread. Wireless telephones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images and the ability to access and browse the internet.

17. In my training and experience, the ready availability and personal nature of wireless telephones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the internet and to distribute, receive and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.

18. Wireless telephones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

Investigation

19. On April 29, 2017, detectives with the Warren County Sheriff's Department were contacted by an anonymous female stating a registered sex offender (Rodney Grant SULLIVAN) had moved and failed to change his sex offender registration.

20. Detective Kevin Talir responded to [redacted] where he made contact with [redacted], who resided at the residence. [redacted] told Det. Talir that SULLIVAN was observed looking at child pornography on [redacted]'s laptop computer. [redacted] was the homeowner of [redacted].

21. On May 4, 2017, I responded to [redacted] with Det. Talir and contacted [redacted] and inquired about what she had observed on her laptop. [redacted] stated she saw "inappropriate" things on her laptop computer since SULLIVAN had been using it. I asked [redacted] to clarify what she meant by "inappropriate". [redacted] said she saw "little kids" doing things with a dog. [redacted] said she allowed SULLIVAN to use her laptop computer and her cellular phone.

22. [redacted] provided me the laptop computer while on scene, and advised she would contact me when she found her cellular phone SULLIVAN was using while living there. [redacted] provided a signed Consent to Search for both the laptop computer and cellular telephone. [redacted] provided the passwords for the devices stating the password was either Rodney or Rodney 1. On May 14, 2017, I was contacted by Det. Talir. Det. Talir said he had received the cellular telephone from [redacted].

23. On or about August 24, 2017, the forensic examination was completed on the laptop computer and cellular phone obtained from [redacted]. The forensic examination of the cellular telephone identified 114 images files that depicted child pornography.

24. On April 25, 2018, I contacted SULLIVAN at his registered residence located at 10224 Big Bend Road St. Louis, Missouri 63112, which is a Hardee's restaurant. I explained what my initial investigation had entailed. SULLIVAN said he had come across child pornography on the Internet. Once he figured out what it was he closed it out.

25. I asked if he had any child pornography on his phone now. SULLIVAN advised he found a website called jailbait which is all over 18.

26. I asked for consent to search his cell phone. SULLIVAN took his cellular phone from the front passenger seat of his vehicle, and provided it to me. The cellular phone was a Samsung SM-J327P. When I looked at the phone, its web browser was on jblover.org. I observed several images similar to the LS Model series of child erotica. Due to the quality and size of the images, I was unable to determine the ages of the females.

27. I navigated to the photo gallery on his device and immediately observed an image of a prepubescent female. The female was standing nude with her legs partially spread displaying her breasts and vagina.

28. I explained to SULLIVAN that I had located an image of child pornography on his device. SULLIVAN said that if he knew it was there he would have deleted it. SULLIVAN advised he obtained all his images from jailbait.com. Although SULLIVAN referred to the site as "jailbait.com," it was later learned through the investigation that the site was "jblover.org."

29. I seized the Samsung, Model Number SM-J327P, silver in color, DEC: 089 869 568 800 424 053, and secured in the St. Charles County Police Department's Evidence Room.

30. On April 25, 2018, I used my office's computer to view the contents of jblover.org website. I observed numerous images of child pornography. Many of the images depicted minor females in various stages of undress.

31. This Affiant knows from training and experience that some people who collect child pornography tend to keep the images they obtain for extended periods of time and do not delete the images. They tend to regard the images as trophies and use them for sexual gratification. They also use the collected images and videos of child pornography as

bargaining tools when trading child pornography with other individuals. Others delete these images knowing they are able to acquire them again with the use of the internet.

32. This Affiant knows from training and experience that some people who collect child pornography utilize mobile devices to store and distribute the files. They also tend to access child pornography from their mobile device to distribute the files in an attempt to avoid detection from Law Enforcement.

Search Methodology to be Employed

33. The examination procedure of electronic data contained in mobile devices, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other examination procedures may be used):

a. examination of all of the data contained in such mobile devices, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment A (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

Conclusion

33. Based upon the above information, information, your affiant asserts that 18 U.S.C. §§2252 and 2252A, which, among other things, make it a federal crime for any person to knowingly possess, receive, and/or distribute child pornography, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment A of this Affidavit, are located on the items seized. I request authority to search such material, specifically, that the Court issue a search warrant.

ANDREW SITTON
Task Force Officer
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 2nd day of May, 2018.

NANNETTE A. BAKER
United States Magistrate Judge
Eastern District of Missouri

ATTACHMENT A

To search the Samsung, Model Number SM-J327P, silver in color, DEC: 089 869 568 800 424 053, including its contents, which cellular telephone is located at St. Charles County Police Department Evidence Room 101 Sheriff Dierker Court O'Fallon, Missouri 63366, for the following:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8)(A) or (C);

2. Any and all electronic device passwords and mobile device passwords and other data security devices designed to restrict access to or hide computer, computer hardware, and mobile device software, documentation, or data. Data security devices may consist of software, or other programming code; and

3. Any and all documents, correspondence, records, e-mails, texts, chats, communications, voicemails, recordings, and internet history pertaining to the production, possession, receipt or distribution of child pornography (or attempt to do so) or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8)(A) or (C).